facebook

February 23, 2011

The Honorable Edward J. Markey
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

The Honorable Joe Barton
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

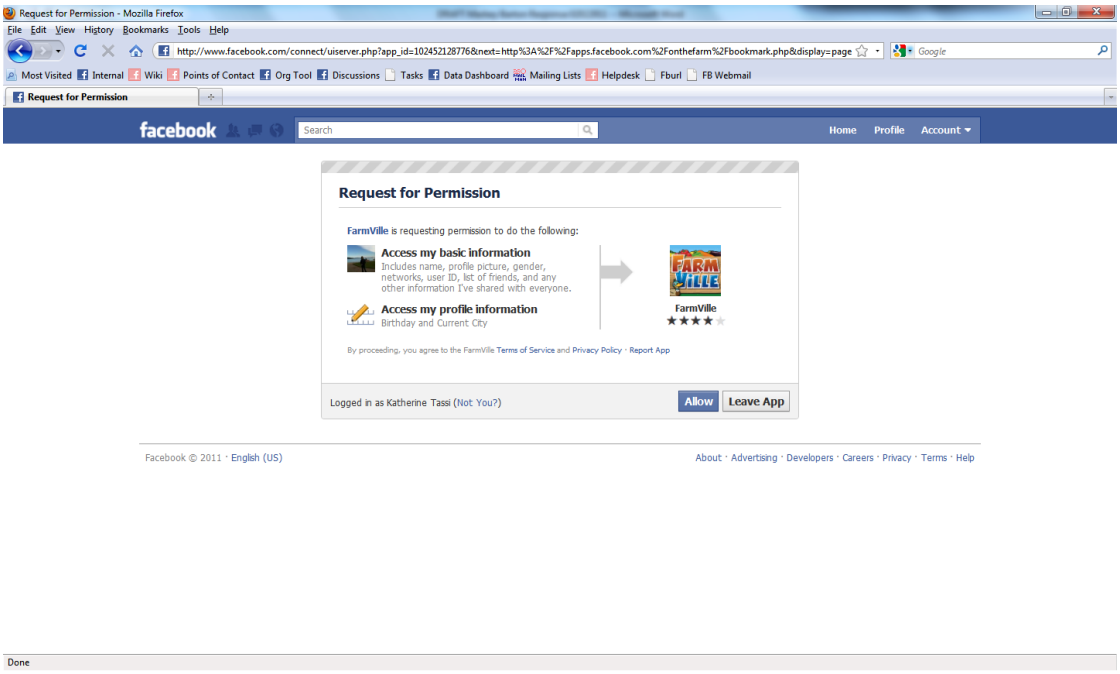
Re: Your letter of February 2, 2011

Dear Congressmen Markey and Barton:

I write to respond to your letter regarding our plans to enable users to grant permission to third-party applications that run on the Facebook platform to access the contact information they have entered on their Facebook profiles.

As an initial matter and by way of background, where third-party applications that run on the Facebook platform request permission from users to obtain access to user information, they do so through a standard permissions screen that identifies for the user the categories of information being requested. For example, a photo-printing application that prints photos for a user requests permission specifically to access a user's photos; a social gaming application that allows users to play a game with his or her friends requests permission to access the user's friends list; a birthday-card application requests permission to access a user's friends' birthdays; a book review application requests permission to access the books a user likes; and so on.

Applications request permission to access these and other categories of information through a standard screen, presented to the user at the moment the user is deciding whether to authorize the application, which identifies precisely what information the application requires to operate. If the user wants to permit the application to obtain access to the information identified, he or she can authorize the application (at which point the application can obtain only the information identified in the permissions screen). If, by contrast, the user is not comfortable sharing the information the application is requesting, the user can decline to authorize the application. A screenshot of a sample permissions screen (one in which the application is asking for permission to access the user's basic information as well as his birthday and current city) is below:

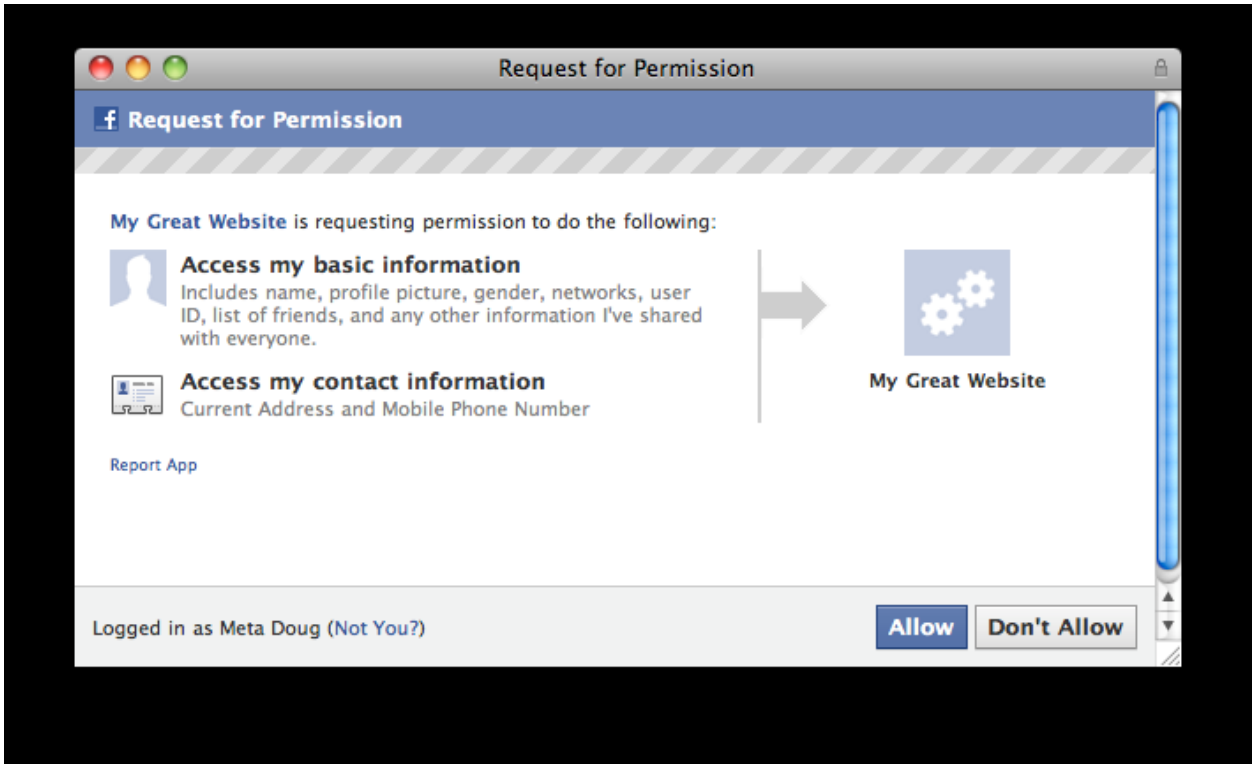


The permissions framework Facebook has deployed for applications has been described as "providing users with simple but real control over their information,"[1] and, after a lengthy investigation, the Office of the Privacy Commissioner of Canada concluded that it adequately informs users regarding what (if any) information they are sharing by choosing to use a given application.[2] The framework is predicated on the assumption that, because users will not typically authorize applications that request access to too much information – indeed, our data show that, on average, each additional category of information an application requests results in a 3% reduction in user click-through rates – applications will not typically ask for more information than they need to operate. After a user authorizes an application to access information from Facebook, the application is subject to technical limitations that prevent it from gaining access to any information beyond that which the user has authorized, and, as we explained in our October 29, 2010, letter to you, it must comply with strict, enforceable terms that limit use of the information it obtains, including outright prohibitions on the sale of user data and/or the direct or indirect transfer of user data to advertising networks or data brokers.[3] Facebook also provides users a tool, under the "Apps You Use" tab in the user's Privacy Settings, that enables users, at any time, to see which applications (if any) have access to which categories of information, and to disable any applications with which the user is not comfortable.

This background helps frame our decision to permit applications to request access to users' contact information. As illustrated, we did not simply grant applications access to users' contact

[1] *See* http://www.cdt.org/blogs/erica-newland/encouraging-steps-privacy-facebook.
[2] *See* http://www.priv.gc.ca/media/nr-c/2010/bg_100922_e.cfm ; *see also* http://www.bbc.co.uk/news/technology-11392454.
[3] *See* https://developers.facebook.com/policy/#policies.

information. We allowed applications to *ask users* for that information, through a permissions screen, represented below, that provided clear and conspicuous notice to the user regarding what information the application is seeking. Nor did we require or encourage users to grant such access. On the contrary, users who considered applications that sought this information had the option to decline the request and continue using Facebook as they had before. Finally, when it appeared that our decision to authorize applications to request this information was causing some degree of concern among users, we suspended the launch and initiated a review that is still underway to enable applications to make innovative use of this category of information, while ensuring that users have ample notice and remain in control of their information.



With this background in mind, we will address each of your questions in turn.

1. **Please describe whether any user information in addition to address and mobile phone number would have been shared with third party application developers under the feature as originally planned. Please also describe whether any of this information was shared prior to Facebook's announcement that it would suspend implementation of the feature.**

Applications that sought access to user contact information had to request such access through the permissions screen described and depicted above. As explained above, once a user authorizes an application by clicking through the permissions screen, Facebook's technology

prevents the application from obtaining user information beyond the categories the user has expressly authorized. Accordingly, to the extent applications that sought access to contact information also obtained access to additional user information, they did so pursuant to the explicit consent of the user.

2. **Please describe what user information will be shared with third party application developers once the feature is re-enabled. Will it be the same information as previously announced prior to the suspension?**

We expect that, once the feature is re-enabled, Facebook will again permit users to authorize applications to obtain their contact information. As noted above, however, we are currently evaluating methods to further enhance user control in this area. For example, we are assessing potential additions to the permissions screen that would appear when an application requests a user's contact information, to determine whether those additions would provide even clearer notice to users regarding the information the application is requesting.

3. **Please describe Facebook's process for developing and vetting the feature referenced above before the feature was suspended.**

Facebook's permissions screen was the result of an extensive product development process that relied on input from virtually every corner of the company. The platform product conceptualized it, the engineering team built it, the user experience team tested it, and the legal, policy, and user operations teams vetted it. In addition, Facebook consulted with numerous third-party privacy groups prior to launch. Decisions to add specific categories of information to the permissions screen are made by the product team, in coordination with the engineering team, with input from other groups as appropriate.

4. **Please describe the process that led Facebook to decide to suspend the rollout of this feature.**

The decision to temporarily suspend the permissions for contact information was sparked by some initial user feedback over the first couple of days that the permission was offered. A key Facebook priority – indeed, one of our foundational principles – is to ensure users can exercise control over their information, and we are always striving to improve the notices we provide to users. On review of the user feedback we received in the wake of the product launch, we determined that we might be able to increase visibility of these categories of data in the permissions screen, and we decided to suspend the feature pending that review. Facebook is committed to providing clear notices to users because we know how important it is for users to trust that they have control over their information.

5. **Please describe the process Facebook is currently employing to adjust the feature prior to re-enabling it.**

We have not yet decided when or in what manner we will re-deploy the permission for mobile numbers and addresses. As noted above, we are evaluating whether and how we can

increase the visibility of applications' requests for permission to access user contact information. We are also considering whether additional user education would be helpful.

6. **In its October 29, 2010 response to us following our Oct. 18, 2010 correspondence on a related matter, Facebook described its internal policies and procedures for ensuring that third party applications satisfy Facebook's terms and conditions. Please describe your internal policies and procedures for ensuring that the new features developed by Facebook comply with Facebook's own privacy policy.**

Facebook's Chief Privacy Counsel is primarily responsible for ensuring that the products and services Facebook offers comply with our privacy policy. This function is performed through extensive product review meetings, during which representatives from Facebook's legal department thoroughly vet new products to determine whether they are compliant with Facebook's privacy policy. The same team administers Facebook's privacy policy to ensure that it provides users with clear notice regarding how Facebook uses their information.

7. **According to Facebook's Developer Blog Post referenced above, the new feature developed by Facebook would permit access to users' addresses and mobile phone numbers to third party application developers and websites. In its Oct. 29, 2010 response to us, Facebook indicated that although it did not believe sharing Facebook User IDs ("UID") with third-party developers involved sharing private user data, it nonetheless understood "the reasons the inclusion of a UID in a referrer URL might make people who use Facebook uneasy, which is why [Facebook is] in the process of making a technical change to address the issue [.]" Please explain why Facebook, while previously acknowledging in its letter to us that sharing a UID could raise user concerns, subsequently considered sharing of a user's home address and mobile phone number – even more sensitive personal information than a UID – to be information that should be more easily accessible to third parties.**

This question is premised on a misunderstanding. Facebook did not determine that a user's contact information should be more easily accessible to third parties than Facebook User IDs. Rather, as explained above, Facebook enabled users to choose to share contact information with applications, by allowing applications to ask users for permission to access that information through our permissions screen. Thus, for example, prior to the launch of this permission, a user that wanted a photo-printing application to send hard copies of photos to his or her home would be required separately to provide his or her address to the application. With the permission in place, the application could ask the user for permission to access his or her address from the user's Facebook profile, and, if the user was comfortable with that request, he or she could grant such access. The same is true for an application that wanted to make use of text messaging, for example, or that identified other, innovative uses of contact information. In all cases, the user remained in control of his or her information. Again, the application was allowed only to ask for permission to access the user's contact information; it was up to the user to determine whether to share it.

8. **If Facebook re-enables this feature, will users who initially opt in to sharing their home addresses and mobile phone numbers be able to have this information subsequently deleted**

by any third party application developer or website that holds it in the event the user no longer wishes to make this information available?

Yes. Our Developer Policies require developers to delete a user's data upon the user's request, and to have an easily accessible mechanism for users to make such a request:

You [the application] will delete all data you receive from us concerning a user if the user asks you to do so, and will provide an easily accessible mechanism for users to make such a request. We may require you to delete data you receive from the Facebook API if you violate our terms.[4]

9. **In an addendum to Facebook's October 29, 2010 response to us, Facebook included a copy of Facebook's privacy policy. In part, that policy stated, "If the changes [to the Privacy Policy] are material, we will provide [users] additional, prominent notice as appropriate under the circumstances." According to news reports, prior to its suspension, the new feature that is planned for re-launch would share user's personal address and mobile numbers.**
    a. **Does Facebook consider this a material change to its privacy policy? If not, why not?**
    b. **Facebook initially announced the new feature in a blog post meant for developers. Does Facebook consider that prominent notice to users? If not, please describe how Facebook intended to notify users of this new feature.**
    c. **Would Facebook's privacy policy have been violated if this new feature had been enabled as originally conceived? If yes, how? If not, why not? If its privacy policy would not have been violated, why did Facebook suspend the rollout of this feature?**

Facebook's privacy policy explains that when a user uses an application that operates on the Facebook platform, the user is "making [his or her] Facebook information available to someone other than Facebook." Allowing applications to request a user's permission to access particular categories of "Facebook information" does not require a change to the Facebook privacy policy.

With respect to notice to users, as explained above, the feature at issue here did not itself provide information to third parties, but rather enabled applications to request permission from users to access users' contact information, through a permissions screen that itself provided notice to users. In addition, also as noted above, Facebook provides users an applications dashboard that enables users to see which applications (if any) have access to which categories of information, and to disable any applications with which the user is not comfortable.

Finally, Facebook temporarily disabled the feature, not because of any concerns regarding compliance with its privacy policy, but rather because, after reviewing user feedback, we determined that we may able to provide even more effective notice through our permissions screen.

10. **Before its decision to enable the new feature, did Facebook consider the risks to children and teenagers posed by enabling third parties to access their home addresses and mobile**

[4] *See* http://developers.facebook.com/policy/#policies.

phone numbers through Facebook? What role did these considerations play in the decision about whether to proceed with the feature's rollout?

Facebook considers risks to minors in all its new product features, and this is no exception, as we are actively considering whether to enable applications to request contact information from minors at all. Insofar as your question asks about minors under 13, Facebook's terms prohibit use of the service by minors under 13, and we employ various technical measures to implement that prohibition.

11. **The January 17, 2010 Facebook Developer Blog Post, stated "As with the other information you share through our permissions process, you need to explicitly choose to share this data before any application or website can access it, and you cannot share your friends' address or mobile number with applications."**
    a. **Given the sensitivity of personal addresses and mobile phone numbers compared to other information users provide Facebook, does Facebook believe the opt-in should be clearer, more prominent, or otherwise distinct from other permissions, commensurate with the sensitivity of this personal information? If yes, please describe how this opt-in will be distinct from other opt-ins. If not, why not?**

As explained above, Facebook is currently considering enhancements to our permissions screen that would highlight for users when they are being asked for permission to share their contact information. Although we do not have details to share at this time, we will keep you apprised of our progress and will advise you of the details if and when we re-enable the feature.

****

Thank you for your inquiry. If we can provide any additional information, please do not hesitate to contact us.

Sincerely,

Marne Levine
Vice President, Global Public Policy